

WHAT IS CLAIMED IS:

1. A method of transferring files over a computer network comprising:
storing a public encryption key and a private encryption key in a client
computer system;
5 sending a request for a data file from said client to a network server; and
in response to said request, (1) checking a file attribute to determine that
said file is to be encrypted with said public encryption key, (2) automatically
retrieving said public encryption key from said client computer system, (3)
encrypting said data file with said public encryption key in said server
10 automatically and without user intervention; and
sending said encrypted data file to said client computer system.
2. A method of storing a data file comprising:
encrypting said data with an encryption key;
storing said encrypted data on a local data storage medium;
15 copying said encrypted data to a remote network server;
storing said data file on a data storage medium in said remote network
server in association with a file attribute that designates said data as encrypted.
3. The method of Claim 2, additionally comprising retrieving said data file
from said network server by a method comprising checking said file attribute prior to
20 routing said data file back to said local data storage medium.
4. A computer network having one or more servers storing data created by
one or more clients, said computer network comprising:
at least one data storage device located on a network server;
at least one data storage device located on a client computer system;
25 data files encrypted with a public key associated with said client
computer system stored on both said network server and said client computer
system, said data files including a file attribute indicating said data files are
encrypted.
5. A method of data storage and retrieval comprising:
30 automatically generating a public key and a corresponding private key in
a client computer system;

storing said public key and said private key in said client computer system;

requesting an unencrypted data file from a network server using said client computer system;

5 requesting said public key from said client computer system automatically and without user intervention;

encrypting, in said network server, said unencrypted data file with said public key to create an encrypted data file;

routing said encrypted data file to said client computer system; and

10 storing said encrypted data file on a storage medium in said client computer system.

6. The method of Claim 5, additionally comprising the step of associating an attribute with said file, said attribute indicating said file is unencrypted when stored on said network server.

15 7. The method of Claim 5, wherein said public key and said private key are based on a password entered by a user when logging on to said client computer system.

8. A computer readable data storage medium having stored thereon commands that are operative to cause a general purpose computer configured as a network server to perform a method of data retrieval comprising the steps of:

20 receiving a request for a data file from a client computer system;

in response thereto, automatically requesting a public key from said client computer system;

automatically encrypting said data file using said public key; and

routing said encrypted data to said client computer system.

25 9. The data storage medium of Claim 8, wherein the method additionally comprises the step of checking a file attribute indicating said file is in unencrypted form prior to performing said encrypting.